Обнаружен новый троян удаленного доступа (RAT), который распространяется через фишинговую кампанию и прячется от механизмов обнаружения с помощью техники «бесфайлового» присутствия.

Исследователи из Prevailion Adversarial Counterintelligence Team (P.A.C.T) прозвали эту малварь DarkWatchman. Собственную C&C-инфраструктуру программа определяет с помощью устойчивого алгоритма генерации доменов (DGA), скрываясь при этом в реестре, через который также незаметно выполняет все свои операции с хранилищем.

Со слов Шермана Смита, исследователя из P.A.C.T:

«Троян задействует новейшие методы реализации бесфайлового присутствия и внутрисистемной активности, а также динамические возможности среды выполнения, такие как самообновление и рекомпиляция. Он демонстрирует очередной шаг в развитии техник бесфайлового присутствия, поскольку все операции временного и постоянного хранения реализует через реестр системы, не прибегая к записи на диск, что позволяет избегать обнаружения большинством средств защиты. Изменения в реестре вполне типичное явление, и бывает трудно определить, какие из них являются аномальными и выходят за рамки обычного поведения системы или ПО».

Как сообщают в Prevailion, среди жертв оказалась одна из российских корпораций, в которой начиная с 12 ноября 2021 года был обнаружен ряд вредоносных артефактов. Сама организация не называется. Учитывая особенности внедрения в систему и долгосрочного присутствия, команда P.A.C.T сделала вывод, что DarkWatchman может использоваться группами хакеров в качестве инструмента проникновения в систему и шпионажа.

Интересным следствием этой новейшей разработки стало то, что она полностью исключает для операторов необходимость найма аффилянтов, на которых обычно возлагается доставка блокирующих файлы вредоносов и последующее извлечение этих файлов. Использование DarkWatchman в качестве первой ступени развертывания вирусов-вымогателей предоставляет его разработчикам лучший надзор над ходом всей операции.
Распространяясь посредством адресных фишинговых писем, маскируемых под уведомление о «завершении срока бесплатного хранения» российской логистической компании Pony Express, DarkWatchman формирует скрытый шлюз для выполнения последующих вредоносных действий. Сама полезная нагрузка трояна содержится в прикрепляемом к письму ZIP-архиве, который преподносится под видом накладной.

По своей сути, DarkWatchman является двухкомпонентным – это и JS-троян, и C#-кейлоггер, последний из которых скрывается от обнаружения в реестре. Оба компонента также чрезвычайно легковесны. JS-код занимает всего 32Кб, а кейлоггер едва дотягивает до 8.5Кб.

«Сохранение двоичного файла в реестре в виде закодированного текста говорит об устойчивом закреплении Darkwatchman, хотя при этом в память диска на постоянную он никогда не записывается. Это также означает, что операторы вредоноса могут обновлять (или заменять) программу при каждом ее выполнении». — сообщили исследователи.

После установки DarkWatchman может запускать произвольные исполняемые файлы, загружать DLL, выполнять JS-код и даже самоликвидироваться с машины. Его JS-подпрограмма также отвечает за закрепление в системе путем создания запланированной задачи, которая запускает вредонос при каждом входе пользователя.

В отчете также говорится, что:

«Сам кейлоггер не сообщается с C&C и не записывает информацию на диск. Вместо этого он пишет лог в ключ реестра, который используется в качестве буфера. В ходе операции троян считывает и очищает этот буфер перед передачей его содержимого на C&C-сервер».

Авторство DarkWatchman еще не установлено, но в Prevailion описали его команду как сильную. При этом исследователи отметили эксклюзивную нацеленность трояна на российские компании, а также орфографические ошибки, обнаруженные в образцах исходного кода, из чего можно сделать вывод, что операторы вряд ли являются в корне англоговорящими людьми.